PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G08B 13/14 — A1

(11) International Publication Number: **WO 99/05659**

(43) International Publication Date: 4 February 1999 (04.02.99)

(21) International Application Number: PCT/US98/14579

(22) International Filing Date: 15 July 1998 (15.07.98)

(30) Priority Data:
08/899,530 24 July 1997 (24.07.97) US

(71) Applicant: CHECKPOINT SYSTEMS, INC. [US/US]; 101 Wolf Drive, P.O. Box 188, Thorofare, NJ 08086 (US).

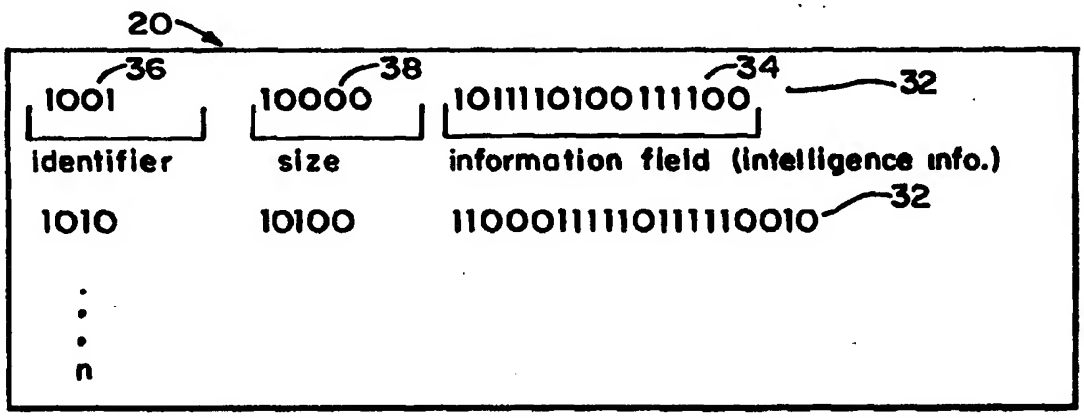
(72) Inventor: BOWERS, John, H.; P.O. Box 401, Clarksburg, NJ 08510–0410 (US).

(74) Agents: KASTEN, Leslie, L. et al.; Panitch Schwarze Jacobs & Nadel, P.C., One Commerce Square, 22nd floor, 2005 Market Street, Philadelphia, PA 19103 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: PROTOCOL FOR STORAGE AND RETRIEVAL OF DATA IN AN RFID TAG WHICH USES OBJECTS



(57) Abstract

An RFID tag (10) stores and retrieves data (34, 36, 38) using objects (32). Each object (32) includes an information field (34) containing intelligence information regarding an item, an identifier code (36) representing the type of intelligence information in the information field, and a size field (38) representing the size of the intelligence information in the information field. An RFID system (22) interrogates an RFID tag (10) by requesting an identifier code (36) for a particular object. If the requested identifier code (36) is present in the RFID tag (10), the tag (10) transmits the information field (34) and size field (38) of the object (32), or the entire object (32). Plural objects (32) may be stored on a single RFID tag (10). The objects (32) are stored in the RFID tag (10) in any desired manner. The same RFID system (22) may use RFID tags (10) with different memory management schemes for storing and retrieving objects (32).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

TITLE OF THE INVENTION

PROTOCOL FOR STORAGE AND RETRIEVAL OF DATA IN AN RFID TAG WHICH USES OBJECTS

BACKGROUND OF THE INVENTION

Electronic article surveillance (EAS) systems for detecting and preventing theft or unauthorized removal of articles or goods from retail establishments and/or other facilities, such as libraries, have become widespread. In general, such security systems employ a security tag which is secured to or associated with an article (or its packaging), typically an article which is readily accessible to potential customers or facility users and, therefore, is susceptible to unauthorized removal. In general, such EAS systems are employed for detecting the presence (or the absence) of a security tag and, thus, a protected article within a surveilled security area or detection zone. In most cases, the detection zone is located at or around an exit or entrance to the facility or a portion of the facility.

One type of EAS system which has gained widespread popularity utilizes a security tag which includes a self-contained, passive resonant circuit in the form of a small, generally planar printed circuit which resonates at a predetermined detection frequency within a detection frequency range. A transmitter, which is also tuned to the detection frequency, is employed for transmitting electromagnetic energy or an interrogation signal into the detection zone. A receiver, tuned to the detection frequency, is positioned proximate to the detection zone. Typically, the transmitter and a transmitter antenna are located on one side of an exit or aisle and the receiver and a receiver antenna are located on the other side of the exit or aisle, so that a person must pass between the transmitter and receiver antennas in order to exit the facility. When an article having an attached security tag moves into or passes through the detection zone, the security tag is exposed to the transmitted energy (the security tag is interrogated), resulting in the resonant circuit of the tag resonating to provide an output signal detectable by the receiver. The detection of such an output signal by the receiver indicates the presence of an article with a security tag within the detection zone and the receiver activates an alarm to alert appropriate security or other personnel.

Existing EAS systems of the type described above and of other types have been shown to be effective in preventing the theft or unauthorized removal of articles.

Security tags of the type described used in a particular store or chain of stores are typically identical. Thus, all articles, regardless of size or value, which include the security tag return an identical signal to the receiver. Recently, passive resonant security tags which return unique or semi-unique identification codes were developed. U.S. Patents Nos. 5,446,447 (Carney et al.), 5,430,441 (Bickley et al.), and 5,347,263 (Carroll et al.) disclose three examples of such security tags. These security tags typically include an integrated circuit to generate the identification code. Such "intelligent" security tags provide additional information about the article detected in the zone of the interrogator. These intelligent security tags typically respond to, and transmit signals, in the radio frequency range, and are known in the art as "radio frequency identification (RFID) tags or "intelligent security tags." RFID tags are used in RFID systems.

To minimize the cost of using RFID tags, it is desired that the cost to produce the tag itself be very low. In many applications, the tags are not reused and thus the entire cost of the tag must be accounted for in the cost of the tagged article. One problem in reducing the cost of making RFID tags is that RFID systems currently in use must rely upon tags having a particular memory configuration, regardless of the application of the tag. This often results in wasted memory space and/or needlessly complex memory configurations.

The actual data stored on a tag will vary according to the specific application. For example, a tag attached to a food product may store identification and freshness data, whereas a tag attached to an electronics product may store only product identification data, such as model number and/or serial number. The wide range of potentially different tag applications makes it difficult to design a single storage and retrieval mechanism for an RFID tag which operates efficiently in the different applications.

Some actual and potential memory configurations are described below, along with their shortfalls:

Pre-allocated memories: The memory locations of the tag are strictly pre-allocated. That is, each bit of data storage is allocated to a particular function. For example, in Fig. 1 of U.S. Patent No. 5,469,363 (Saliga), the tag has an EEPROM memory which is segmented with a predetermined string of bytes. Each grouping of bytes performs a different function (e.g., lock, identification, trace). Since the memory locations are strictly pre-allocated, it is not possible to use this tag in an application that may require different types of information. Also, if some of the pre-allocated functions are not required, it is still necessary to provide a memory segment for the unused functions.

Directory allocated memories: It may be possible to emulate the memory architecture of computer hard drives, wherein a directory would store the location and identification of each block of information stored in the

memory of the tag, as well as the location of unallocated memory. When it is desired to write new information to the memory, the new information would be written to the appropriate locations.

One inherent limitation to using this type of memory allocation scheme in RFID tags is that the number of bits of information required to perform a transaction (i.e., to access a tag) is relatively large. For example, the entire contents of the directory must first be read by the interrogator before the location and/or contents of specifically desired information stored in the memory of the tag can be read or written. For tags with large memories, the directory information itself can be much larger than the size of the information desired to be read or written. In RFID tag systems, and particularly where many tags may be within the read or write zone of the interrogator, this relatively high number of bits required to perform a transaction limits the number of tags that can be accessed per unit time. Speed limitations on information transferring also arise because only selected RF channels may be used in RFID systems, as determined by regulations from governmental authorities (e.g., Federal Communications Commission) who allocate radio spectrum bands, or as determined by system architecture requirements.

Another inherent limitation to using a directory allocated memory scheme in an RFID tag is that it is difficult to limit access to the tag information, when limited access is desired. In intelligent tags that are used for retail or rental operations, it may be necessary to

store information about the tagged article for which limited access is desired. Limiting access to certain stored information will prevent unauthorized persons from gaining access to the information which may then be used for illicit purposes. For example, information may be stored on the tag which indicates current ownership of the tagged article (e.g., article is owned by the store, or article has been sold and is owned by the customer). If access to this information was obtained by an unscrupulous person, the ownership information could be changed, or the ownership information could be extracted from a legitimately sold article and then stored into other like unsold articles in the possession of the retailer. Then, the unsold articles could be removed from the retailer without payment and without the RFID system generating an alarm because the tags associated with the articles would contain information indicating that they had already been sold.

A directory allocated memory scheme has no effective means for limiting access to information. While a scheme exists to hide a directory entry, this scheme has an inherent weakness which is a result of a related feature of directory schemes wherein any part of the memory can be directly accessed. The directory stores information related to the location of all information blocks, including hidden directory entries. One need only directly address such locations to find the hidden entries. It is relatively easy to read all of the memory locations within the tag, and by using the unhidden directory information, determine the

complete contents of the tag, including the hidden information.

Other schemes are available to limit access to stored information. For example, a lock and key mechanism may be used wherein access to information would require a "password" of some type (the key) to "unlock" the access door. This scheme would be too easy to defeat if used with intelligent tags. By merely monitoring the transactions between the intelligent tag and the interrogator at the point of sale, a thief could determine the password for accessing a particular block of information. Furthermore, if a lock and key mechanism was used, extra circuitry would have to be included on the intelligent tag to ensure that memory locations protected by a password are unreadable, except after the password has been given. This extra circuitry would increase the cost and complexity of the tag.

Encryption could be used to protect information on an intelligent tag. Encryption offers better security than password key systems. Encryption uses mathematical techniques to re-map information in a way that is difficult to decode without a key. One encryption approach would be to select a particular encryption mechanism for the RFID system and use it for some or all of the information to be transferred between the tag and the interrogator. This approach has the problem that, ultimately, the encryption mechanism will be understood and therefore of no utility over time.

Another encryption approach involves dynamically setting the encryption means by using one or more non-

constant keys. This approach is traditionally used in "smart cards" for which a very high degree of security is required. Unfortunately, data encryption and decryption circuitry is relatively expensive, and thus not practical for use with disposable intelligent tags.

Yet another encryption approach might be to store encrypted data in memory using the previously described directory system. However, this approach also has its drawbacks because encrypted data takes up many more bits than unencrypted data. Thus, this approach also has the negative impact of increasing the cost and complexity of the tag.

Despite the wide variety of techniques that may used to store information in the memory of RFID tags in a manner which protects the information from being read by unauthorized persons or from being improperly altered, there is still a need for a tag memory management technique which minimizes data storage and transfer requirements, is flexible, is inexpensive to implement, and yet provides adequate security against most attempts to defeat it. The present invention fulfills such needs by "objectizing" the information to be stored in the memory of the tag and transferred between the tag and the interrogator. That is, the information to be stored and transferred is identified and managed by the tag as a group of information blocks or objects, each of which can be uniquely identified.

BRIEF SUMMARY OF THE INVENTION

The present invention provides a memory for a radio frequency identification (RFID) tag. The memory includes one or more objects. Each object includes an information field containing intelligence information regarding an item, an identifier code representing the type of intelligence information in the information field, and a size field representing the size of the intelligence information in the information field.

One embodiment of the invention provides a security tag associated with an item. The security tag includes an integrated circuit having a memory for storing one or more objects and for outputting one or more of the objects as a response signal upon interrogation of the security tag by a selected interrogation signal. Each object includes an information field containing intelligence information regarding the item, an identifier code representing the type of intelligence information in the information field, and a size field representing the size of the intelligence information in the information field.

Another embodiment of the invention provides an RFID surveillance system for using the RFID tag.

Another embodiment of the invention provides a method for communicating between an interrogator of a surveillance system and a security tag associated with an item. The security tag includes an integrated circuit having a memory for storing one or more objects. Each object includes an information field containing intelligence information regarding the item, an identifier code

representing the type of intelligence information in the information field, and a size field representing the size of the intelligence information in the information field. The method comprises the steps of transmitting a request signal from the interrogator which contains an object identifier code, receiving the request signal in a security tag, searching the security tag memory to determine whether the requested object is stored therein, and transmitting at least the information field and the size field of the requested object if the requested object is stored in the security tag memory. The transmission is received by the interrogator.

Another embodiment of the invention provides a protocol for interaction between an interrogator of a surveillance system and a security tag associated with an item. The security tag includes an integrated circuit having a memory for storing one or more objects. Each object includes an information field containing intelligence information regarding the associated item, an identifier code representing the type of intelligence information in the information field, and a size field representing the size of the intelligence information in the information field. The method comprises the steps of transmitting a control message from the interrogator which contains an object identifier code, receiving the control message in a security tag, searching the security tag to determine whether the object to which the object identifier code pertains is stored in the security tag, and performing a control function if the object is stored in the security

tag. The control function may be to cause the security tag to transmit the object, to delete the object from its memory, to alter its memory so that the object cannot be deleted, or to change the contents of the information field of the object stored in its memory.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing summary, as well as the following detailed description of preferred embodiments of the invention, will be better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, there are shown in the drawings embodiments which are presently preferred. It should be understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown. In the drawings:

Fig. 1 is a block diagram schematic of a security tag suitable for use with the present invention;

Fig. 2 is a functional block diagram schematic of an interrogator suitable for use with the present invention;

Fig. 3 is a representation of the contents of a memory for the security tag of Fig. 1 for storing one or more objects;

Fig. 4 is a functional block diagram of a sample memory for the security tag of Fig. 1 showing a memory allocation scheme for storing one or more objects;

Fig. 5 is a sample correlation table which relates object identifier codes with their corresponding intelligence information;

Figs. 6A and 6B are schematic block diagrams of first and second system environments for using the security tag of Fig. 1 having one or more objects stored thereon; and

Fig. 7 is a flowchart of a process for detecting whether a security tag has been subjected to tampering.

DETAILED DESCRIPTION OF THE INVENTION

Certain terminology is used herein for convenience only and is not be taken as a limitation on the present invention. In the drawings, the same reference numerals are employed for designating the same elements throughout the several figures.

Fig. 1 shows general details of a sample RFID tag 10 suitable for use with the present invention. The security tag 10 includes a passive resonant radio frequency (RF) circuit 12 for use in detecting when the tag 10 is within a zone monitored by a reader or interrogator, as is well-known in the art. One well-known type of circuit 12 has a coil antenna 14 and a capacitor 16 which together form a resonant circuit with a predetermined (operational) resonant frequency (i.e., the selected radio frequency). Power for the security tag 10 is derived from the antenna 14 in a conventional manner. Furthermore, the security tag 10 includes an integrated circuit (IC) 18 for providing "intelligence" to the security tag 10. The IC 18 is

connected to the circuit 12. The IC 18 includes a programmable memory 20, as described below, for storing bits of identification or other data. The IC 18 outputs a data stream comprised of stored data when sufficient power is applied thereto. In one embodiment of the invention, the data stream creates a series of data pulses by switching an extra capacitor (not shown) across the coil antenna 14 for the duration of the data pulses. This changes the resonant frequency of the RF circuit 12, detuning it from the operational frequency. Thus, instead of the RF circuit 12 returning a simple response signal at a single operational resonant frequency, it returns a modulated signal containing a packet of preprogrammed information from the memory 20. The packet of information (data pulses) is received and processed by interrogator receiving circuitry and is decoded (if necessary) to provide identification and/or other information about the tagged article. Other methods of using the data in the IC memory 20 to output identification data from the security tag 10 are within the scope of the invention. The IC 18 is preferably also a passive device and is powered in the same manner as the RF circuit 12 (i.e., by using energy received at the antenna 14 from the interrogator transmitter signal). The security tag 10 is thus a so-called RFID tag. Other types of RFID tags may be used with the present invention. Examples of other RFID tags which have circuitry suitable for use as part of the circuitry of the security tag 10 are shown in U.S. Patents Nos. 5,446,447 (Carney et al.), 5,430,441 (Bickley et al.), and 5,347,263 (Carroll et al.).

Fig. 2 is a block diagram schematic of a typical reader or interrogator 22 suitable for use with the security tag 10 of Fig. 1. The interrogator 22 and the security tag 10 communicate by inductive coupling, as is well-known in the art. The interrogator 22 includes a transmitter 24, receiver 26, antenna assembly 28, and data processing and control circuitry 30, each having inputs and outputs. The output of the transmitter 24 is connected to a first input of the receiver 26, and to the input of the antenna assembly 28. The output of the antenna assembly 28 is connected to a second input of the receiver 26. A first and a second output of the data processing and control circuitry 30 are connected to the input of the transmitter 24 and to a third input of the receiver 26, respectively. Furthermore, the output of the receiver 26 is connected to the input of the data processing and control circuitry 30. Interrogators having this general configuration may be built using circuitry described in U.S. Patents Nos. 3,752,960, 3,816,708, 4,223,830 and 4,580,041, all issued to Walton, all of which are incorporated by reference in their entirety herein. The physical implementation of the interrogator 22 is dictated by the specific application (e.g., taking, inventory, monitoring an exit, checking out). Two known implementations of interrogators 22 which are suitable for use with the present invention are a pair of smart pedestals (not shown) and a hand-held RF-ID scanner.

In the preferred embodiment of the invention, a predefined set of security tags 10 are prepared to be associated with a predefined items. More specifically, the

security tags 10 are prepared to be associated with, and applied to a predefined set of articles (not shown), unique or semi-unique security tag information is assigned to each security tag 10, the security tags 10 are programmed accordingly, and the security tags 10 are attached directly to each article or to the packaging of each article. Alternatively, the tags 10 may be programmed after they are applied to the articles. In the disclosed embodiment, one security tag 10 is associated with each article.

Fig. 3 is a block diagram of non-volatile memory allocation in the memory 20 of a tag 10 which depicts information blocks or objects 32 stored in the memory 20 of the tag 10. Each object 32 includes at least a data field or information field 34 containing intelligence information regarding the tagged article, an identifier code 36 representing the type of intelligence information in the information field 34, and a size field 38 representing the size of the intelligence information in the information field 34. In some applications, only one object 32 is stored in the memory 20. In other applications, two or more objects 32 are stored in the memory 20. Each object 20 has a unique identifier code 36. The maximum number of objects 32 which can be stored in a tag 10 is limited solely by the size of the memory 20 and the size of the objects 32.

In the example shown in Fig. 3, the identifier code 36 is four bits in length, allowing for sixteen different identifier codes 36. In a commercially suitable embodiment of the invention, the identifier code 36 may be of some other size such as a thirty-two bit code. In the

first object 32, the information field 34 has a length of sixteen bits, so the size field 38 is a binary sixteen or "10000". In the second object 32, the information field is twenty bits in length, so the size field 38 is a binary twenty, or "10100". The length of the information field 34 may vary from object to object, both within a single tag, and from tag to tag. Fig. 3 shows both identifier codes 36 as having the same number of bits. For a given system of RFID tags and interrogators, the length of the identifier codes 36 and size fields 38 are preferably constant (i.e., all tags 10 in a given system preferably have identifier codes 36 and size fields 38 of the same bit length). However, the lengths of identifier codes 36 and size fields may vary from system to system. Variable bit length identifier codes 36 and size fields 38 are within the scope of the invention, but are not preferred because they increase the complexity of the data storage scheme, the tag interrogation procedure and the object retrieval process.

In prior art tag memory allocation schemes, such as illustrated in Fig. 4 of U.S. Patent No. 5,469,363 (Saliga et al.), a consecutive string of memory locations are used to store tag data. In the present invention, it is not necessary to store the object 32 as a consecutive string of data bits or bytes. Furthermore, the object 32 may be compressed and thus may not resemble the actual information if viewed in compressed form. Thus, Fig. 3 merely shows the type of data stored in the tag's memory 20, not the preferred manner of organizing or storing the data therein.

Fig. 4 shows an example of a memory allocation scheme for storing one or more objects 32 in a tag memory 20. The approach in Fig. 4 is a modified version of the prior art linked list data structure. In Fig. 4, the memory 20 contains five objects 32 stored in consecutive rows of memory space, each object including an identifier code 36 (ID), a size field 38 (SZ) and an information field 34 (INF). An optional end of data field 39 (EOD) may be placed at the end of the last stored object 32. Memory is allocated from left to right and from top to bottom. When searching the memory 20 for a particular object, the memory manager (not shown) examines each of the ID and SZ fields 36, 38. Beginning at the upper left of the memory 20, each ID field 36 is compared with the identifier code of the object being searched for. If they are not the same, the memory manager increments a pointer by the sum of the sizes of the ID, SZ and INF fields, respectively, to point to the ID field of the next object 32, i.e., toward the right and downward. (The size of the INF field is obtained from the SZ field.) The process is repeated until an ID field matches the one being searched for, or until the last object has been examined (as indicated, for example, by reaching the EOD field 39, failing to locate another ID field after a predetermined period of time, or by any other suitable means).

When an object 32 is added to the memory 20 of Fig. 4, it is always added to the end of the linked list. If an EOD field 39 is used, it is moved to the end of all the objects 32. When an object 32 is deleted from the

memory 20 of Fig. 4, all of the objects 32 which follow the deleted object are moved back in space so that no gaps are left between consecutive objects 32.

The memory allocation scheme of Fig. 4 may also be modified to store plural objects 32 in nonconsecutive memory locations even though such a scheme may reduce the storage efficiency and increase the complexity of the object search.

Fig. 5 is a sample correlation table 40 which relates identifier codes 36 to intelligence information associated with respective information fields 34. For example, identifier code "1001" may be associated with an information field 34 containing the expiration date of the tagged article (e.g., 12/30/97 or 01/06/98) whereas identifier code "1010" may be associated with an article owner (e.g., store X or purchasing consumer Y). Data in the information field 34 may be fixed or locked, such as in the case of an expiration date, or it may be changeable, such as in the case of an article owner. The ability to change data stored in a memory of a tag 10 is well-known, and thus is not described further in detail. In Fig. 5, data in the information field 34 represents one piece of intelligence information. However, it is within the scope of the invention to represent more than one piece of intelligence information within a single information field 34. Also, the number of bits or bytes in the information field 34 may exceed the number necessary to store the desired intelligence information. Thus, the information field 34 may be four bytes, even though it may be possible to code

the ownership or expiration date information in less than four bytes.

Referring again to Fig. 3, only two pieces of information are required for memory management of each object 32, the identifier code 36 and the size field 38. As discussed above, the identifier code 36 is required to uniquely identify each of the objects 32 stored on the tag 10. The size field 38 is required to understand how to delimit the object 32 so that the information field 34 can be properly extracted. The size field 38 may also optionally be used for allocating space in the tag's memory 20.

To store intelligence information on a tag 10, such as when the tag 10 is initially brought into service and attached to an article, the following steps are performed:

(1) An entire object 32 is sent to the tag 10 by an interrogator 22. The parts of the object 32 may be sent in any order as long as there is a way to properly delimit the various parts within the tag's memory 20.

(2) The tag 10 determines whether it can store the object 32. If so, the object 32 is stored and an acknowledgment message is returned to the interrogator 22. The interrogator 22 does not control how the object 32 is stored within the tag 10, nor does the tag 10 communicate such information back to the interrogator 22. If the tag 10 cannot store the object 32, a failure message is returned to the interrogator 22.

Preferably, the object 32 is encoded for extra security and/or for error detection and correction. The encoding step may involve adding extra, redundant bits of information to the object 32 which may or may not be stored in the tag's memory 20.

To read information from a tag 10, the following steps are performed.

(1) Interrogator 22 sends out a signal asking the tag 10 to transmit a particular object. For example, the signal may ask the tag 10 to transmit its date object (i.e., the object having identifier code 1001). The signal may be continuously transmitted, or may be transmitted only once, or a discrete number of times.

(2) If the tag 10 contains a date object, the tag 10 preferably responds by transmitting the entire date object 32. Alternatively, the tag 10 responds by transmitting only the information field 34 and size field 38 of the object 32. If the tag 10 does not contain a date object, a failure message or some other type of predetermined message is returned to the interrogator 22. Alternatively, no tag transmission occurs and the absence of a transmission is interpreted by the interrogator 22 as meaning that no such object 32 exists on the tag 10.

Step (1) of the reading process may be preceded by an interrogator control message asking whether a particular object 32 is stored on a tag 10. If a positive response is received, the process would then continue as described above.

When reading out an object 32 from a tag 10, the identifier code 36 and size field 38 are preferably read out before the information field 34. This is because the size of the information field 34 is unknown until the size field 38 is decoded. Knowing the size of the information field 34 is useful in determining when transfer of the information field 34 is completed. However, the parts of the object 32 may be transmitted in any order as long as there is a way to properly delimit the various parts.

Figs. 6A and 6B are block diagram schematics of an RFID system using tags 10 with objects stored therein. In Fig. 6A, a computer 42 sends control signals to, and receives RFID tag data from, the interrogator 22. The computer 42 accesses the database table 40 when necessary. In Fig. 6B, the database table 40 is incorporated into the interrogator 22.

The use of objects allows for selected actions to be requested by the interrogator 22 and for selected control functions to be performed by the tag 10 in response to the request. The interrogator request may be viewed as a control message. The control message includes an object identifier code 36. One such control message is to request that the tag 10 transmit an object 32 having the particular identifier code 36. Another control message is to request that the tag 10 respond affirmatively if it contains the requested object 32, without actually sending the object. Another control function may be to delete the object 32 from the tag's memory 20. Yet another control function may be to change the contents of the information field 34 of a

particular object 32, such as to indicate that ownership of the article to which the tag is secured has passed from the store to the consumer. Yet another control function may be to lock the object 32 in the tag's memory 20, such as by altering the memory 20 of the tag 10 so that the object 32 cannot be altered or deleted. Other control functions are within the scope of the invention.

Storing data in a tag 10 as described above has significant advantages over existing tag data storage techniques. One major advantage is that the memory allocation scheme of the tag 10 is invisible to the interrogator 22. That is, the interrogator 22 has no knowledge (and needs no knowledge) about how data is stored within the memory 20 of the tag 10 to communicate with the tag 10 and perform desired actions with respect to the tag data. The internal operation of the tag's IC 18 is thus hidden and separate from the information transfer operations. One benefit of this fact is that neither the interrogator 22, nor its protocol, have to be changed for different tag applications. This independence allows the designer to incorporate features into the tag's IC 18 without having to change the remaining parts of the RFID system, or the interrogator/tag communication protocol. For example, data compression may be added to the tag's IC 18 to reduce the number of stored memory bits without even requiring the interrogator 22 to know that data compression is performed. Data compression is particularly attractive when RFID tags are used in applications which require storage of large amounts of data.

The tag/interrogator communication protocol may be simplified, compared to systems that use the directory approach for managing data. A minimum of extra data is transferred while communicating between the interrogator 22 and the tag 10 compared to the directory approach.

Another advantage of the tag 10 is that different types of tags 10 may be used with the same interrogator 22. One particular tag implementation may manage the objects 32 as a linked list. Another tag implementation may use a directory allocated memory, as described above. The choice of which approach to use would depend upon the desired cost and complexity of the tag's memory 20.

Yet another advantage of the tag 10 is that different tag designs having different applications may be used with the same RFID system. Since the tag 10 has its own object memory manager, data is stored independent of the interrogator protocol. For example, referring to Figs. 3 and 5, one type of tag 10 may be used in a retail food store for coding expiration dates on food articles in the information field 34. This tag's object 32 may have an identifier code 36 of 1001 and may manage the object using a linked list approach. Another type of tag 10 may be used in a retail consumer product store for tracking article ownership. This tag's object 32 may have an identifier code 36 of 1010 and may manage the object using a directory approach. Despite the completely different memory management schemes, the same interrogator 22 may be used for communicating with both types of tags 10.

Alternatively, by merely modifying the interrogation protocol, the tag design for completely different applications may be identical, even though the tags may have information fields 34 and size fields 38 of different bit lengths. Further, completely different tag designs may be used for the same application by merely using the same identifier code 36 in both types of tags. This flexibility reduces the cost of developing a product line of tags which are used in disparate applications, and also ensures that new designs of tags are compatible with existing RFID systems. In contrast, data stored in the memory of tags using a fixed memory allocation scheme must be arranged in a predetermined manner to be compatible with other RFID systems. In a fixed scheme, any change in the tag or application may require costly changes to other parts of the RFID system.

If desired, the size field 38 may be used to manage the allocation of the tag's memory 20 for storing objects 32, thereby maximizing the use of limited memory space. A sixteen bit information field 34 need only take up sixteen bits of memory space, as illustrated in Fig. 4. In contrast, a conventional fixed memory allocation scheme designates a fixed sized block for data, even if the data requires less space. Since the fixed sized block must be selected to accommodate the largest expected data string, memory space will be wasted whenever the data string is smaller than the maximum allowed string.

Yet another advantage of the tag 10 is that information stored on the tag 10 can be reasonably well

hidden, without having to rely on encryption techniques. Encryption is costly, expensive, and adds to transaction time.

Consider the following situation wherein the information field **34** is the date of sale. If an article is unsold, there is no date of sale and the information field **34** has a default value representing that fact (e.g., 00/00/00). When an article is legitimately purchased, a date of sale is placed in the information field **34**. The interrogator **22** is set to trip an alarm only when a tagged article is detected in the interrogation zone which has no date of sale or which has a date of sale which differs from the then current date.

A sophisticated thief wants to obtain information stored on the RFID tag of a legitimately purchased article. Since the article was legitimately purchased, the information field **34** now contains intelligence information indicating an actual date of sale. If the thief discovers how to get into the contents of the information field **34**, the thief may be able to reprogram the tag **10** of an unpurchased article (which is still in the store) so that the information field **34** indicates a date of sale. The thief may then walk past the interrogator **22** and out of the store while carrying the article, without triggering any alarms. In the present system, the thief must first discover the identifier code **36** for the date of sale. An identifier code **36** may be a 24 bit string. Since the thief initially has no way of knowing what the identifier code **36** is, the thief would have to try to read all possible objects

32 within the tag 10 and try to infer, after reading them, which one has the date of sale information. To do so, the thief requests the object 32 having identifier code 000000000000000000000000 (for which there may or may not be an object 32), then 000000000000000000000001, then 000000000000000000000010, then 000000000000000000000011, then 000000000000000000000100, and so on, until the thief has requested all of the objects with identifier codes 36 through 111111111111111111111111. After cycling through all of the identifier codes 36, the thief will have discovered some objects, maybe even only one. At this stage, it will be relatively easy for the thief to deduce which object 32 contains the date of sale information. However, because there are 24 bits in an identifier code 36, the thief will has to read 2^{24} different objects, or 67,108,864 different objects, to get to this point.

Assuming that it takes about 10 milliseconds to read each object 32 (or to find out that the requested object does not exist), the thief can attempt to read 100 objects per second. At this rate, it will take 671,089 seconds, which is equivalent to 186 hours or 7.77 days, to read all possible objects in the tag.

To inhibit discovery of the object information, the store may adopt a policy of periodically changing the identifier code 36. One week it may be 101110010100010110111010. The next week it may be 010110101110100110101101. If the store changes the identifier code 36 for the date of sale on a weekly basis, the code

will change faster than a thief could discover it. For example, if the identifier code 36 is a 32 bit number, and the thief can read as many as 1000 objects per second, it will still take about 4 billion attempts, which will take over a month, to read all of the data.

By constantly changing the identifier code 36, tags 10 may be checked to ensure that the identifier code 36 matches the appropriate date(s) of sale. For example, an identifier code 36 of 10111001010000101101111010 may correlate with dates of sale from 12/15/96 to 12/22/96, whereas an identifier code 36 of 01011010111010011010110 1 may correlate with dates of sale from 12/23/96 to 12/30/96. Even if a thief discovered a particular identifier code 36, as well as the coding scheme for encoding the date of sale, the thief would still have to know which dates are appropriate for the particular identifier code 36. If the thief programs a tag 10 with a date outside of the range correlated with the particular identifier code 36, an alarm would trigger at a store interrogator. If a thief programmed a tag 10 with a date that is within the proper range, but is not the current date, the RFID system may optionally be programmed to trigger an alarm to alert store personnel that the tagged article is either a previously purchased article (e.g., an article being returned), or an illegally programmed or tagged article. Store personnel would have to further investigate to determine which scenario exists.

To further thwart object discovery, the format of the information field 34 may be also changed as a function of time.

To further prevent the information on the tag 10 from being discovered and subjected to tampering, one object 32 on the tag 10 may be linked to another object on the tag 10.

Consider the situation wherein two objects 32_1 and 32_2 are stored on each tag of a set of tags 10 used on articles in a retail store environment. The first object 32_1 is the date of sale, as described above. The date of sale may be useful in determining if the article was actually purchased, or whether a warranty on the tagged article is still in effect. The second object 32_2 is the date of last physical inventory. The store conducts frequent inventory checks, such as once a week, and updates object 32_2 with the latest date during each inventory check. When an article is sold, the date of sale is recorded in object 32_1. For every sold article, there will be a predetermined relationship between the date in object 32_1 and the date in object 32_2. In the example of weekly inventory checks, the two dates should never be more than seven days apart.

Assuming now that a sophisticated thief discovered how to manipulate the first object 32_1. The thief can now insert sale dates to make an unsold article appear to be sold (to shoplift the article, as discussed above), or to make an article sold a long time ago appear to be recently sold (to bring a broken article within a warranty period, or

to return an article after the return period has expired). However, the thief is not necessarily aware that the first object 32_1 must be corroborated with a second object 32_2 to avoid triggering an alarm or alerting the store to a discrepancy. Thus, the thief may manipulate the first object 32_1 in a manner that is inconsistent with the second object 32_2 and the stored corroboration therebetween. For example, the thief may change the first object 32_1 so that the sale date of an article that actually sold on 2/15/96 now reads 2/15/97, while being unaware that the date of last physical inventory is also stored on the tag **10** and reads 2/13/96. Since the time between the actual sale date and the last inventory check should always be seven days or less, and the article being returned shows a date difference of more than one year, the store knows that the tag **10** may have been subjected to tampering. Object linking thus can be used to thwart the efforts of even sophisticated thieves or insiders who may learn how to read and alter selected objects **32**.

Fig. 7 is a flowchart of the basic process for detecting whether a tag **10** having two or more linking objects **32** was subjected to tampering. Two or more objects **32** are read from a tag **10** (step 100). Next, data is retrieved which defines the linkage between the plural objects **32** (step 200). The data may be stored in an interrogator, external computer, or in the tag **10** itself. Next, the linkage is checked to see if it is still intact (step 300). If not, an alarm condition is indicated (step 400) and store personnel investigates the matter in detail.

One implementation of this process is to use a comparator in the interrogator or store computer to retrieve linkage or corroboration data from a memory location. The comparator checks that the information fields 34 of the linked objects 32 bear the appropriate relationship therebetween. Other implementations of object linkage are within the scope of the invention.

As described above, the security tags 10 are associated with predefined items in the form of articles, and the tags 10 are attached directly to each article or to the packaging of each article. This embodiment of the invention is useful for an RFID system. Alternatively, the invention may be used in other types of systems which use security tags 10. Some examples include a library checkout system having tagged library articles, a personal identification system wherein persons wear tagged badges and obtain access to selected areas based upon information stored in their badges, and a baggage handling system wherein luggage is individually tagged.

It will be appreciated by those skilled in the art that changes could be made to the embodiments described above without departing from the broad inventive concept thereof. It is understood, therefore, that this invention is not limited to the particular embodiments disclosed, but it is intended to cover modifications within the spirit and scope of the present invention as defined by the appended claims.

CLAIMS

1. A memory for a radio frequency identification (RFID) tag, the memory including one or more objects, each object including:

(i) an information field containing intelligence information regarding an item;

(ii) an identifier code representing the type of intelligence information in the information field; and

(iii) a size field representing the size of the intelligence information in the information field.

2. A security tag associated with an item, the security tag including an integrated circuit having a memory for storing one or more objects and for outputting one or more of the objects as a response signal upon interrogation of the security tag by a selected interrogation signal, each object including:

(i) an information field containing intelligence information regarding the item;

(ii) an identifier code representing the type of intelligence information in the information field; and

(iii) a size field representing the size of the intelligence information in the information field.

3. A security tag associated with and attached to an item, the security tag including:

(a) a resonant circuit for use in detecting the presence of the item by receiving an interrogation signal and returning a response signal, and

(b) an integrated circuit connected to the resonant circuit, the integrated circuit having a memory for storing one or more objects and adapted to output one or more of the objects as the response signal upon interrogation of the security tag by a selected interrogation signal, each object including:

(i) an information field containing intelligence information regarding the item;

(ii) an identifier code representing the type of intelligence information in the information field; and

(iii) a size field representing the size of the intelligence information in the information field.

4. A surveillance system comprising:

(a) a security tag associated with and attached to an item, the security tag including:

(i) a resonant circuit for use in detecting the presence of the item by receiving an interrogation signal and returning a response signal, and

(ii) an integrated circuit connected to the resonant circuit and having a memory for storing one or more information blocks and for outputting one or more of the information blocks as the response signal upon interrogation of the security tag by a selected interrogation signal, each information block including

intelligence information regarding the item, an identifier code representing the type of intelligence information in the information block, and a size code representing the size of the intelligence information;

(b) an interrogator for outputting the selected interrogation signal and receiving the response signal;

(c) a computer connected to the interrogator for directing the interrogator to output a selected interrogation signal and for interpreting the response signal, the computer accessing a table of identifier codes and respective types of intelligence information.

5. A surveillance system according to claim 4 wherein the memory stores two information blocks, and the computer further comprises a memory for storing data representing an expected relationship between the two information blocks, and a comparator for comparing the two information blocks to determine whether the expected relationship exists.

6. A method for communicating between an interrogator of a surveillance system and a security tag associated with an item, the security tag including an integrated circuit having a memory for storing one or more objects, each object including an information field containing intelligence information regarding the item, an identifier code representing the type of intelligence information in the information field, and a size field

representing the size of the intelligence information in the information field, the method comprising the steps of:

(a) transmitting a request signal from the interrogator, the request signal containing an object identifier code;

(b) receiving the request signal in a security tag;

(c) searching the security tag memory to determine whether the requested object is stored therein; and

(d) transmitting at least the information field and the size field of the requested object if the requested object is stored in the security tag memory, the transmission being received by the interrogator.

7. The method according to claim 6 wherein step (d) comprises transmitting the entire requested object if the requested object is stored in the security tag.

8. A protocol for interaction between an interrogator of a surveillance system and a security tag associated with an item, the security tag including an integrated circuit having a memory for storing one or more objects, each object including an information field containing intelligence information regarding the associated item, an identifier code representing the type of intelligence information in the information field, and a size field representing the size of the intelligence

information in the information field, the method comprising the steps of:

(a) transmitting a control message from the interrogator, the control message containing an object identifier code;

(b) receiving the control message in a security tag;

(c) searching the security tag to determine whether the object to which the object identifier code pertains is stored in the security tag; and

(d) performing a control function if the object is stored in the security tag.

9. The method according to claim 8 wherein the control function is for the security tag to transmit the object.

10. The method according to claim 8 wherein the control function is to delete the object from the memory of the security tag.

11. The method according to claim 8 wherein the control function is to alter the memory of the security tag so that the object cannot be deleted.

12. The message according to claim 8 wherein the control function is to change the contents of the information field of the object stored in the memory of the security tag.

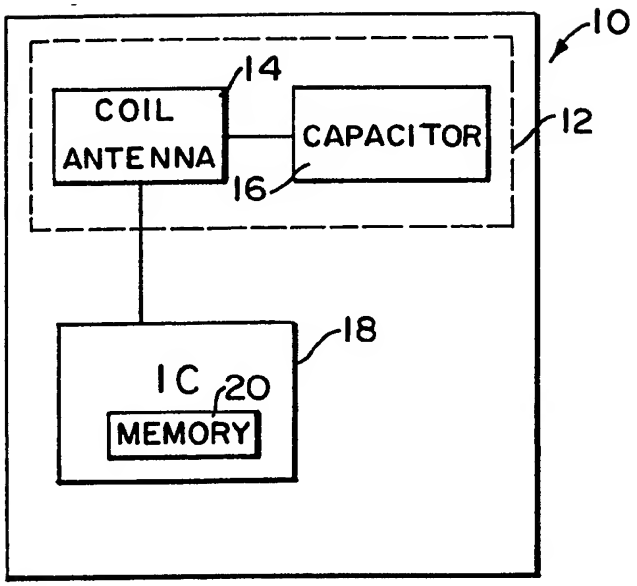

10
14
COIL ANTENNA
CAPACITOR
12
16
18
IC
20
MEMORY

FIG. 1

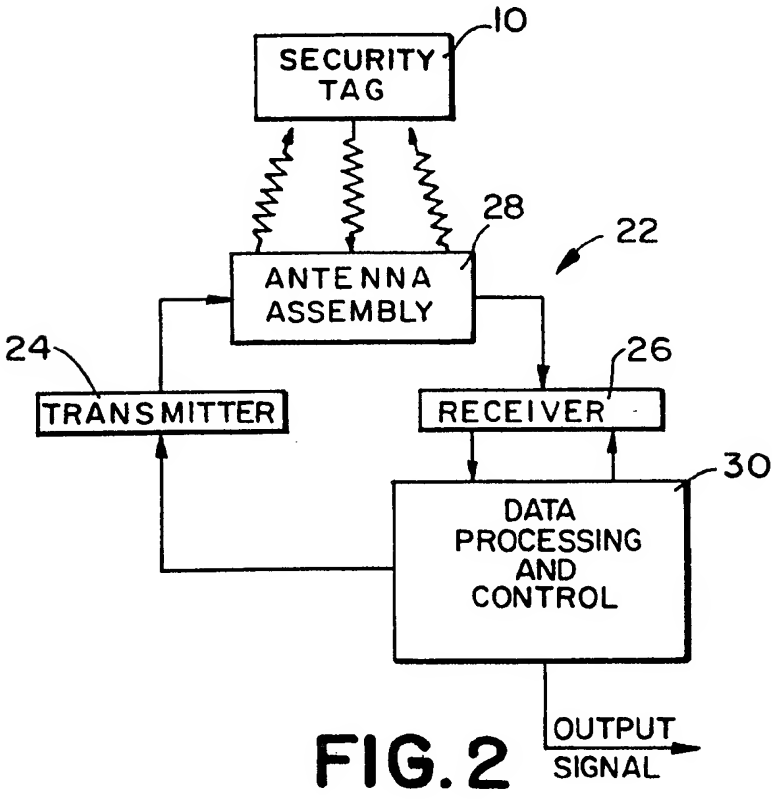

10
SECURITY TAG
28
22
ANTENNA ASSEMBLY
24
26
TRANSMITTER
RECEIVER
30
DATA PROCESSING AND CONTROL
OUTPUT SIGNAL

FIG. 2

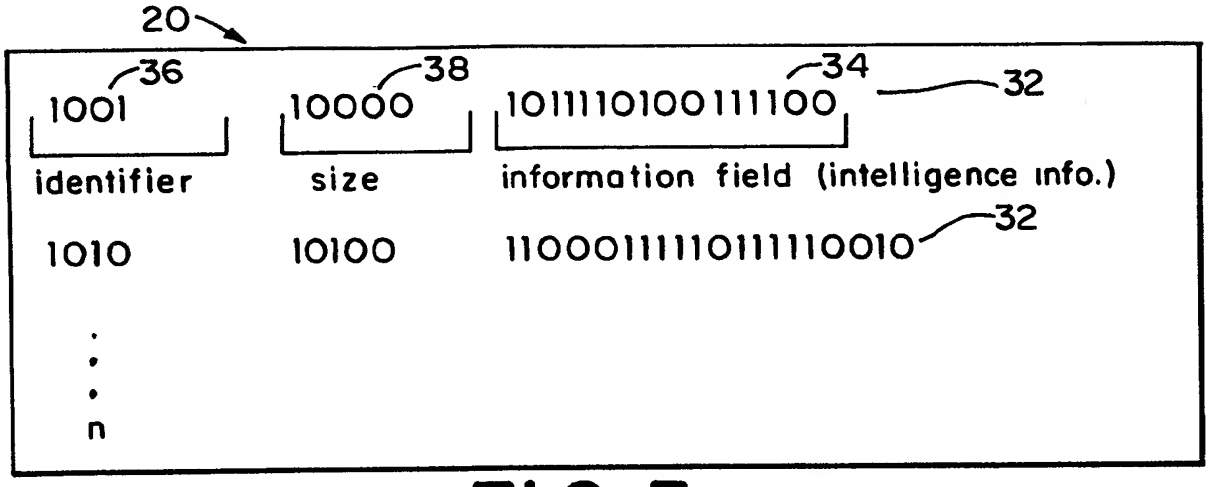


FIG. 3

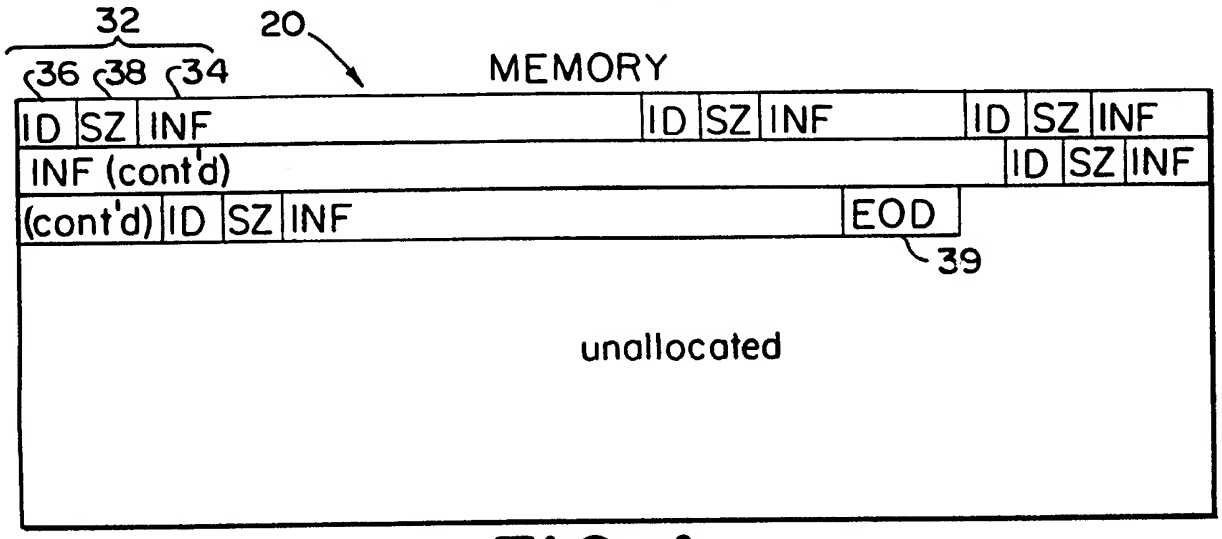


FIG. 4

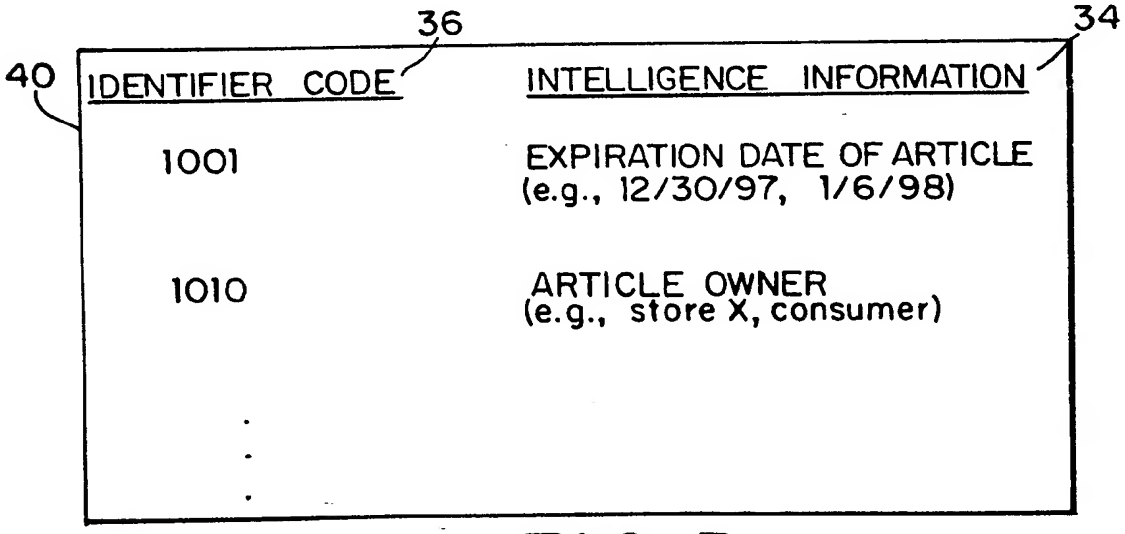


FIG. 5

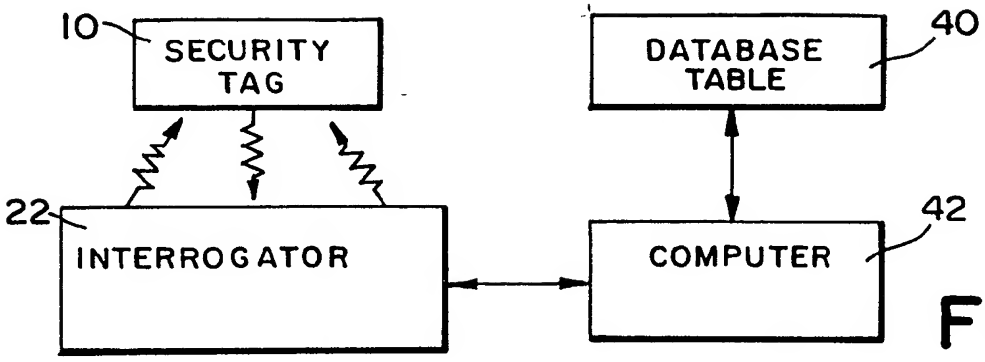


FIG. 6A

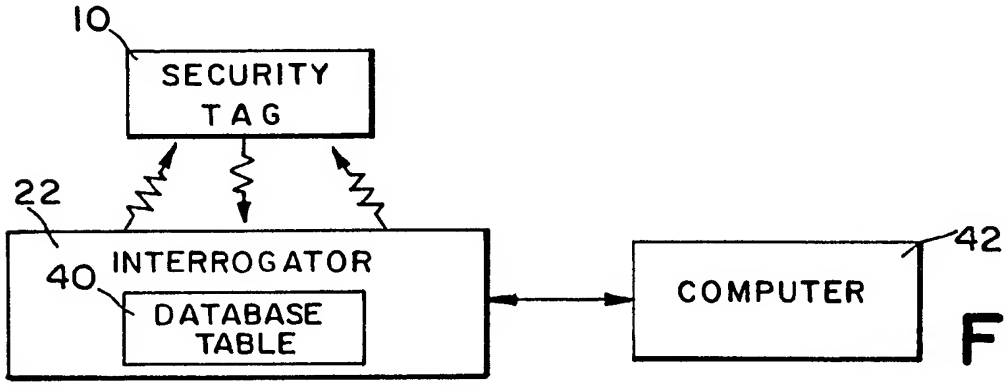


FIG. 6B

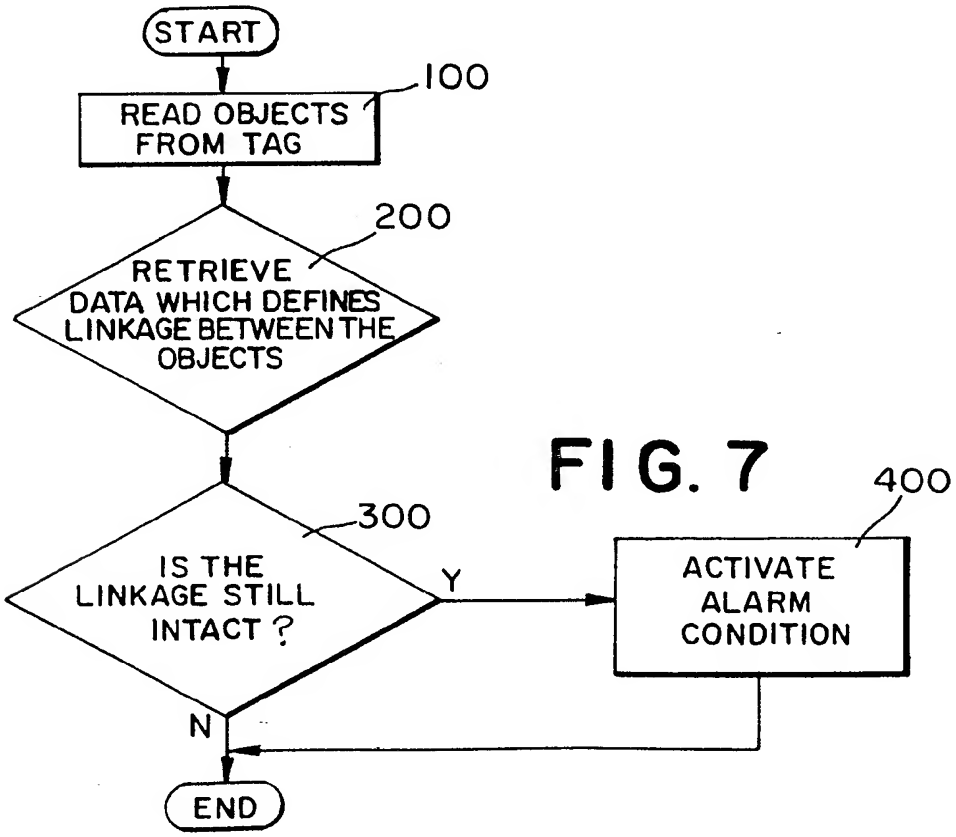


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/14579

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G08B 13/14
US CL :340/572.1; 711/163
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 340/572.1, 571, 568.6, 552; 711/163, 164

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

none

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,469,363 A (SALIGA) 21 November 1995, abstract, Figures 1-5, and col. 1, line 52 to col. 12, line 17.	1-12
Y	US 4,713,753 A (BOEBERT et al) 15 December 1987, Figures 3-7 and col. 7, line 52 to col. 10, line 27.	1-12
Y	US 5,113,344 A (KELLOGG et al) 12 May 1992, abstract, Figures 1-3 and col. 2, line 42 to col. 8, line 34.	1-12
A	US 5,745,036 A (CLARE) 28 April 1998, abstract and Figures 1-7.	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 13 SEPTEMBER 1998	Date of mailing of the international search report 19 OCT 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer SIHONG HUANG Telephone No. (703) 305-4700

Form PCT/ISA/210 (second sheet)(July 1992)*